UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/553,984	10/20/2005	Hideo Sato	273868US6PCT	1022

22850 7590 04/06/2009

OBLON, SPIVAK, MCCLELLAND MAIER & NEUSTADT, P.C.
1940 DUKE STREET
ALEXANDRIA, VA 22314

EXAMINER
KING, JOHN B

ART UNIT	PAPER NUMBER
2435	

NOTIFICATION DATE	DELIVERY MODE
04/06/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patentdocket@oblon.com
oblonpat@oblon.com
jgardner@oblon.com

Office Action Summary	Application No.	Applicant(s)	
	10/553,984	SATO, HIDEO	
	Examiner	Art Unit	
	John B. King	2435	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 December 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-3,6-8 and 11-16* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3,6-8 and 11-16* is/are rejected.

7)☒ Claim(s) *13* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This office action is in response to applicant's amendment filed on December 3, 2008.

2. Claims 1-3, 6-8, and 11-16 are pending in this application. Claims 1-3 and 6-8 are amended by applicant's amendment. Claims 4, 5, 9, and 10 have been cancelled and Claims 11-16 have been added. The limitations of claim 5 have been included in independent claims 1 and 6.

3. Applicant's arguments in respect to the new issues of Claims 1-3, 6-8, and 11-16 have been considered but they are not persuasive.

Response to Arguments

4. The amendment to the specification is accepted as overcoming the objection of the specification of the first Office Action, mailed September 3, 2008.

5. The amendment to claims 2, 3, 7, and 8 are accepted as overcoming the rejections under 35 U.S.C. 112, second paragraph of the first Office Action. However, these claims are now rejected under 35 U.S.C. 112 second paragraph for new reasons based upon the amended claims.

6. The amendment to claims 4 and 9 are accepted as overcoming the rejections under 35 U.S.C. 112, second paragraph for lack of antecedent basis of the first Office Action as claims 4 and 9 have been cancelled by applicant's amendment.

7. Applicant's arguments filed December 3, 2008 have been fully considered but they are not persuasive. In the remarks applicant argues:

I) Bjorn does not teach the limitations of claims 1, 4, 6, and 9.

II) Bjorn in view of Buttiker does not teach the limitations of claims 5 and 10. Bjorn in view of Buttiker does not teach imaging an inside portion of a target as biometric data.

III) Shinzaki and Lee, whether taken individually or in combination with Bjorn, fail to supply the claimed features lacking in the disclosure of Bjorn.

In response to applicant's arguments:

I, II and III) Applicant is arguing that the rejection of the first Office Action does not teach the limitations of the amended claims. The claims in the application have been amended in such as way as to allow new art be used in this rejection because of the change in the scope of the claimed invention. Therefore, the applicant's arguments are considered moot based upon the new grounds of rejection as set forth below.

Examiner Notes

8. Examiner cites particular columns and line numbers in the references as applied to the claims below for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested that, in preparing responses, the applicant fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the examiner.

Claim Objections

9. Claim 13 is objected to because of the following informalities: The claim depends upon itself. The examiner believes that this is a typographic error and that the claim should properly depend upon claim 1. Appropriate correction is required.

Claim Rejections - 35 USC § 112

10. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

11. **Claims 1, 2, 6, 7, and 11** are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

As per claims 1, 6, and 11, the claims teach performing analog to digital conversion on the variation patterns signal to generate an encryption key that is used later to encrypt the image data. However, the written description or the claims themselves do not explain in detail how the key is generated to allow someone of ordinary skill in the art to make the invention. The description and claims state that the A/D conversion is used in the key generation by use of a prescribed algorithm in

combination with the hamming distances, but no details have been provided as to **HOW** the key is generated after the hamming distances have been calculated.

As per claims 2 and 7, the claims teach using hamming distance to generate an encryption key. However, the written description or the claims themselves do not explain in detail how the key is generated to allow someone of ordinary skill in the art to make the invention. The description and the claims state that the hamming distance is used to generate the key, but no details have been provided as to **HOW** the key is actually generated. The hamming distance is being used but no information has been provided to show how it is used or **WHY** it's different than using any other number to generate a key.

As per claims 2 and 7, the claims teach performing the hamming distance between the image data and the evaluation patterns. However, the written description teaches performing the hamming distance between the variation patterns and the evaluation patterns. This is considered as new matter.

12. Claims **1, 2, 6, 7, and 11** are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention.

As per claims 1, 6, and 11, the claims teach performing analog to digital conversion on the variation patterns signal to generate an encryption key that is used

later to encrypt the image data. However, the written description or the claims themselves do not explain in detail how the key is generated to enable one of ordinary skill in the art to make the invention. The description and claims state that the A/D conversion is used in the key generation by use of a prescribed algorithm in combination with the hamming distances, but no details have been provided as to **HOW** the key is generated after the hamming distances have been calculated.

As per claims 2 and 7, the claims teach using hamming distance to generate an encryption key. However, the written description or the claims themselves do not explain in detail how the key is generated to enable one of ordinary skill in the art to make the invention. The description and the claims state that the hamming distance is used to generate the key, but no details have been provided as to **HOW** the key is actually generated. The hamming distance is being used but no information has been provided to show how it is used or **WHY** it's different than using any other number to generate a key.

13. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

14. **Claims 2, 3, 7, 8, and 14-16** are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 2 and 7 recites the limitation "the different evaluation patterns". There is insufficient antecedent basis for this limitation in the claim. It is unclear if the “different evaluation patterns” and the “predetermined evaluation patterns” are the same.

Claims 2 and 7 also teach using hamming distance being used to generate an encryption key, but does not specifically teach how the key is generated. It is unclear if the hamming distance is the encryption key or if it used as a seed for the key generation or something else.

Claims 3 and 8 recites the limitations “the evaluation patterns” and also “selecting evaluation patterns”. It is unclear if the “different evaluation patterns” and “the predetermined evaluation patterns” from claims 2 and 7 are the same as “the evaluation patterns” of claims 3 and 8.

Claims 14-16 teach using different types of elements (piezoelectric, active, and passive) as the second signal. However, claim 1 teaches the second signal having variation patterns. It is unclear to the examiner how the signal output from these elements can contain these variation patterns that are specific to the imaging device. If the second signal is the output from a touch pad, how does that contain a variation pattern? According to the written description, pages 8-10, the variation patterns come from an image of the internals of the imaging device without a target, a finger, present. Then, on page 17, these other types of elements are listed as a different embodiment of the invention.

15. The examiner has cited particular examples of 35 U.S.C. 112 rejections above. It is respectfully requested that, in preparing responses, the applicant check the claims for further 35 U.S.C. 112 rejections as being indefinite in case it was inadvertently missed by the examiner. The following prior art rejections are based upon the examiner's best interpretation of the claims.

Claim Rejections - 35 USC § 103

16. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

17. **Claims 1-3, 6-8, and 11-16** are rejected under 35 U.S.C. 103(a) as being unpatentable over Bjorn (US Patent No. 6035398, published March 7, 2000) in view of Wuidart et al. (US Pre-Grant Publication 2003/0103629 A1, filed October 10, 2002) hereinafter referred to as Wuidart and further in view of Rowe et al. (US Pre-Grant Publication 2002/0009213 A1, published January 24, 2002) hereinafter referred to as Rowe.

As per claim 1, Bjorn discloses an encryption device for encrypting information on a confidential target, comprising: an imaging unit configured to perform imaging on a target and to output a signal **(Bjorn, col. 3 lines 25-35, teaches extracting a fingerprint from a user and sent to the temporary storage unit.)**; an identification

unit configured to perform analog/digital conversion on the first signal having the image data to create identification information **(Bjorn, col. 3 lines 25-35, teaches extracting certain features from the fingerprint and storing this information in a temporary storage unit. If all of these actions are occurring, the analog signal has to be converted to a digital signal.)**; a creation unit configured to perform analog/digital conversion on the second signal having the variation patterns to create encryption key information **(Bjorn, col. 3 lines 25-60, teaches using a hash of the fingerprint data to generate a key. Also, the analog to digital conversion is inherent in this case because the signal has to be converted before use.)**; and an encryption unit configured to encrypt the identification information by using the encryption key information **(Bjorn, col. 4 lines 4-20, teaches that the user's biometric data, fingerprint, can be encrypted. If the data is encrypted it must be encrypted using an encryption key.)**

However, Bjorn does not specifically teach outputting a variation patterns signal that is specific to the imaging unit or using these variation patterns to generate an encryption key. Bjorn also does not specifically teach the imaging unit imaging an inside portion of a target.

Wuidart discloses outputting said second signal including variation patterns specific to the imaging unit **(Wuidart, paragraphs 11-13, teaches having a physical parameter of a network be used to revoke a key for that device.)**

Bjorn and Wuidart are analogous art because they are from the same field of endeavor of key management.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Bjorn by adding the teachings of Wuidart because this would allow the use of a physical parameter of the system in key management. This will prevent unauthorized access because the physical parameter cannot easily be copied **(Wuidart, paragraph 4.)**

However, Bjorn in view of Wuidart does not teach using the variation patterns to generate an encryption key.

Although, Bjorn does teach using a hash of the user's fingerprint to generate a key. This is using one signal to generate a key instead of using a different signal. It would have been obvious to one of ordinary skill in the art at the time the invention was made to use one signal instead of another to generate the encryption key.

However, Bjorn in view of Wuidart also does not teach the biometric data that is used being from an inside portion of a target.

Rowe discloses said first signal including image data of an inside portion of the target **(Rowe, paragraph 8, teaches that blood vessel patterns can be used as biometric information.)**

Bjorn and Rowe are analogous art because they are from the same field of endeavor of using biometric data for user authentication.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to use one form of biometric data, such as blood vessel patterns, instead of using another form of biometric data, such as fingerprints.

As per claim 2, Bjorn in view of Wuidart and further in view of Rowe discloses The encryption device according to claim 1 **[See rejection to claim 1 above]**, wherein the creation unit includes a storage unit configured to store a plurality of predetermined evaluation patterns having different hamming distances, and said creation unit is further configured to create the encryption key information by using at least one calculated hamming distance of the image data and the different evaluation patterns **(Bjorn, col. 4 lines 4-37, teaches storing fingerprint templates in a memory. These templates are later hashed and used to generate a key.)**

Although Bjorn in view of Wuidart and further in view of Rowe does not specifically teach the use of hamming distance to generate the key it would have been obvious to one of ordinary skill in the art at the time the invention was made. Calculating the hamming distance between two sets of bits is well known in the art as well as generating a key from a number, such as a random number or seed. The hamming distance is just a number and a hash is also just a number. Unless there is a specific reason to use the hamming distance, see 112 rejection above, it would have been obvious to use a random number or anything else such as a hash to generate the key.

As per claim 3, Bjorn in view of Wuidart and further in view of Rowe discloses The encryption device according the claim 2 **[See rejection to claim 2 above]**, further comprising: a communication unit configured to communicate with a prescribed communication party, and the creation unit is further configured to select evaluation patterns requested by the communication party, from the evaluation patterns stored in the storage unit **(Bjorn, col. 8 lines 30-40, teaches communicating with a**

certification authority in order to transfer a fingerprint template for user authorization.)

As per claim 6, Bjorn discloses An encryption method for encrypting information on a confidential target, comprising: performing analog/digital conversion on the first signal having the image data to create identification information **(Bjorn, col. 3 lines 25-35, teaches extracting certain features from the fingerprint and storing this information in a temporary storage unit. If all of these actions are occurring, the analog signal has to be converted to a digital signal.)**; performing analog/digital conversion on the second signal having the variation patterns to create encryption key information **(Bjorn, col. 3 lines 25-60, teaches using a hash of the fingerprint data to generate a key. Also, the analog to digital conversion is inherent in this case because the signal has to be converted before use.)**; and encrypting via a processor the identification information by using the encryption key information **(Bjorn, col. 4 lines 4-20, teaches that the user's biometric data, fingerprint, can be encrypted. If the data is encrypted it must be encrypted using an encryption key.)**

However, Bjorn does not specifically teach outputting a variation patterns signal that is specific to the imaging unit or using these variation patterns to generate an encryption key. Bjorn also does not specifically teach the imaging unit imaging an inside portion of a target.

Wuidart discloses outputting a second signal that includes variation patterns specific to the imaging unit **(Wuidart, paragraphs 11-13, teaches having a physical parameter of a network be used to revoke a key for that device.)**

Bjorn and Wuidart are analogous art because they are from the same field of endeavor of key management.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Bjorn by adding the teachings of Wuidart because this would allow the use of a physical parameter of the system in key management. This will prevent unauthorized access because the physical parameter cannot easily be copied **(Wuidart, paragraph 4.)**

However, Bjorn in view of Wuidart does not teach using the variation patterns to generate an encryption key.

Although, Bjorn does teach using a hash of the user's fingerprint to generate a key. This is using one signal to generate a key instead of using a different signal. It would have been obvious to one of ordinary skill in the art at the time the invention was made to use one signal instead of another to generate the encryption key.

However, Bjorn in view of Wuidart also does not teach the biometric data that is used being from an inside portion of a target.

Rowe discloses said first signal including image data of an inside portion of the target **(Rowe, paragraph 8, teaches that blood vessel patterns can be used as biometric information.)**

Bjorn and Rowe are analogous art because they are from the same field of endeavor of using biometric data for user authentication.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to use one form of biometric data, such as blood vessel patterns, instead of using another form of biometric data, such as fingerprints.

As per claim 7, Bjorn in view of Wuidart and further in view of Rowe discloses The encryption method according to claim 6 **[See rejection to claim 6 above]**, further comprising: storing a plurality of predetermined evaluation patterns having different hamming distances; and creating the encryption key information including calculating at least one hamming distance of the image data and the different evaluation patterns **(Bjorn, col. 4 lines 4-37, teaches storing fingerprint templates in a memory. These templates are later hashed and used to generate a key.)**

Although Bjorn in view of Wuidart and further in view of Rowe does not specifically teach the use of hamming distance to generate the key it would have been obvious to one of ordinary skill in the art at the time the invention was made. Calculating the hamming distance between two sets of bits is well known in the art as well as generating a key from a number, such as a random number or seed. The hamming distance is just a number and a hash is also just a number. Unless there is a specific reason to use the hamming distance, see 112 rejection above, it would have been obvious to use a random number or anything else such as a hash to generate the key.

As per claim 8, Bjorn in view of Wuidart and further in view of Rowe discloses The encryption method according to claim 7 **[See rejection to claim 7 above]**, further

comprising: selecting evaluation patterns requested by a prescribed communication party from the evaluation patterns being stored **(Bjorn, col. 8 lines 30-40, teaches communicating with a certification authority in order to transfer a fingerprint template for user authorization.)**

As per Claim 11, Bjorn discloses An encryption device for encrypting information on a confidential target, comprising: imaging means for performing imaging on a target and outputting a first and second signal **(Bjorn, col. 3 lines 25-35, teaches extracting a fingerprint from a user and sent to the temporary storage unit.)**; identification means for performing analog/digital conversion on the first signal having the image data to create identification information **(Bjorn, col. 3 lines 25-35, teaches extracting certain features from the fingerprint and storing this information in a temporary storage unit. If all of these actions are occurring, the analog signal has to be converted to a digital signal.)**; creation means for performing analog/digital conversion on the second signal having the variation patterns to create encryption key information **(Bjorn, col. 3 lines 25-60, teaches using a hash of the fingerprint data to generate a key. Also, the analog to digital conversion is inherent in this case because the signal has to be converted before use.)**; and encryption means for encrypting the identification information by using the encryption key information **(Bjorn, col. 4 lines 4-20, teaches that the user's biometric data, fingerprint, can be encrypted.)**

However, Bjorn does not specifically teach outputting a variation patterns signal that is specific to the imaging unit or using these variation patterns to generate an encryption key. Bjorn also does not specifically teach the imaging unit imaging an inside portion of a target.

Wuidart discloses said second signal including variation patterns specific to the imaging means **(Wuidart, paragraphs 11-13, teaches having a physical parameter of a network be used to revoke a key for that device.)**

Bjorn and Wuidart are analogous art because they are from the same field of endeavor key management.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Bjorn by adding the teachings of Wuidart because this would allow the use of a physical parameter of the system in key management. This will prevent unauthorized access because the physical parameter cannot easily be copied **(Wuidart, paragraph 4.)**

However, Bjorn in view of Wuidart does not teach using the variation patterns to generate an encryption key.

Although, Bjorn does teach using a hash of the user's fingerprint to generate a key. This is using one signal to generate a key instead of using a different signal. It would have been obvious to one of ordinary skill in the art at the time the invention was made to use one signal instead of another to generate the encryption key.

However, Bjorn in view of Wuidart also does not teach the biometric data that is used being from an inside portion of a target.

Rowe discloses said first signal including image data of an inside portion of the target **(Rowe, paragraph 8, teaches that blood vessel patterns can be used as biometric information.)**

Bjorn and Rowe are analogous art because they are from the same field of endeavor of using biometric data for user authentication.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to use one form of biometric data, such as blood vessel patterns, instead of using another form of biometric data, such as fingerprints.

As per claim 12, Bjorn in view of Wuidart and further in view of Rowe discloses The encryption device according to claim 1 **[See rejection to claim 1 above]**, wherein said imaging unit is further configured to project near-infrared light into the target **(Rowe, paragraph 8, teaches using near-infrared light, to image blood vessels in a targets hand.)**

As per claim 13, Bjorn in view of Wuidart and further in view of Rowe discloses The encryption device according to claim 1 **[See rejection to claim 1 above]**, wherein the first signal includes blood vessel pattern information representing a formation pattern of blood vessel tissues inside the target **(Rowe, paragraph 8, teaches using near-infrared light, to image blood vessels in a targets hand.)**

As per claim 14, Bjorn in view of Wuidart and further in view of Rowe discloses The encryption device according to claim 1 **[See rejection to claim 1 above]**, wherein said second signal includes data based on a signal output from a piezoelectric element

of a touch pad **(Wuidart, paragraphs 11-13, teaches using a physical parameter of a network.)**

As per claim 15, Bjorn in view of Wuidart and further in view of Rowe discloses The encryption device according to claim 1 **[See rejection to claim 1 above]**, wherein said second signal includes data of a group of active elements **(Wuidart, paragraphs 11-13, teaches using a physical parameter of a network.)**

As per claim 16, Bjorn in view of Wuidart and further in view of Rowe discloses The encryption device according to claim 1 **[See rejection to claim 1 above]**, wherein said second signal includes data of a group of passive elements **(Wuidart, paragraphs 11-13, teaches using a physical parameter of a network.)**

Conclusion

18. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

19. Any inquiry concerning this communication or earlier communications from the examiner should be directed to John B. King whose telephone number is (571)270-7310. The examiner can normally be reached on Mon. - Fri. 7:30 AM - 4:00 PM est..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571)272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/JBK/
/Kimyen Vu/
Supervisory Patent Examiner, Art Unit 2435